Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

POR MEDIO DE LA CUAL SE ACTUALIZAN LAS POLÍTICAS, ESTANDARES DE SEGURIDAD Y USO DE RECURSOS INFORMÁTICOS EN INDEPORTES ANTIOQUIA

EL GERENTE DEL INSTITUTO DEPARTAMENTAL DE DEPORTES DE ANTIOQUIA en uso de atribuciones legales, en especial las conferidas por la Ordenanza Departamental 8E del 1° de marzo de 1996, y

CONSIDERANDO:

1. Que la importancia de los activos de la información y de su valía en la operación y en la gestión de la Entidad, como medio para alcanzar los objetivos estratégicos propuestos y concibiendo que las TIC´s traen inmersas grandes amenazas.

2. Que se deben implementar mecanismos para garantizar el cumplimiento de la normatividad vigente en materia de Derechos de autor y de la protección de la información y los datos.

3. Que los cambios en la configuración de la plataforma tecnológica de la Entidad hacen necesario la actualización de estas políticas.

En mérito de lo anterior,

RESUELVE

ARTÍCULO 1. OBJETIVO GENERAL:

Implementar el Sistema de Gestión de Seguridad de la Información en INDEPORTES ANTIOQUIA, determinando las políticas de seguridad de la información y uso de recursos informáticos, con el fin de proteger la información contra una gran variedad de amenazas, minimizando el riesgo y asegurando la continuidad del servicio, acorde a los lineamientos definidos por el Departamento Administrativo de la Función Pública, el Ministerio de las TIC y el programa de Gobierno Digital.

ARTÍCULO 2. DEFINICIÓN DE POLÍTICA DE SEGURIDAD INFORMÁTICA (PSI):

Las políticas institucionales son directivas con aceptación general, que constituyen un canal formal de actuación de los usuarios, en relación con los recursos y servicios tecnológicos disponibles en INDEPORTES ANTIOQUIA.

La PSI constituye los procedimientos y compromisos de la Entidad, que le permiten actuar proactivamente ante situaciones que comprometan la integridad de los activos de información.

Las políticas por sí solas no constituyen una garantía para la seguridad, estas deben responder a intereses y necesidades organizacionales, que lleven a un esfuerzo conjunto de sus actores para administrar sus recursos y reconocer en los mecanismos de seguridad de la información, factores que faciliten la formalización y materialización de los compromisos adquiridos entre los usuarios y la Entidad.

ARTÍCULO 3. ALCANCE:

Estas políticas están dirigidas al personal interno de la Entidad (servidores públicos, contratistas, entrenadores, deportistas, así como también a los residentes de las Villas deportivas: Antonio Roldán Betancur, Villa Náutica y CEDEP Urabá, Neiva-80). También aplica a personas externas (usuarios no frecuentes y visitantes) el alcance de dichos lineamientos.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

Todo usuario de los recursos tecnológicos en INDEPORTES ANTIOQUIA, tiene un grado de responsabilidad a partir del momento que tiene autorización de acceso a la información y a los equipos o hace uso de los canales de comunicación Institucionales. Por tanto, los usuarios deberán conocer y aceptar estas directrices y el desconocimiento de este documento no exonera a la persona de las responsabilidades adquiridas.

Además de las políticas generales dispuestas a cumplir en INDEPORTES ANTIOQUIA, se adoptarán las estrategias para la seguridad de la información definidas en la NTC ISO 27001:2013, y las que la Entidad disponga a partir del análisis de los riesgos de la seguridad de la Información.

ARTÍCULO 4. OBJETIVO ESPECÍFICO:

El objetivo de este documento es implementar el sistema de gestión de seguridad de la información, bajo la reglamentación del uso de los recursos tecnológicos, con el fin de incentivar mejores prácticas para su uso, minimizar los riesgos en materia de seguridad de la información y adoptar un código de conducta eficaz, con espíritu de autorregulación para el manejo y aprovechamiento de los recursos tecnológicos Institucionales.

Por lo tanto, la Entidad implementará, operará, monitoreará, revisará y mejorará permanentemente el sistema de gestión de seguridad de la información, en el contexto de su propia seguridad, para las actividades globales institucionales, de cara a los riesgos, buscando minimizar los impactos en la Entidad, en caso de cualquier tipo de interrupción de los servicios TIC.

Entre otras, la Entidad propende por:

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores de la Entidad, practicantes, contratistas y demás actores participes de la operación de la Entidad.
- Velar por la continuidad de los procesos de la Entidad.
- Minimizar los riesgos asociados a la seguridad de la información.
- Cumplir con los lineamientos establecidos por el Departamento Administrativo de la Función Pública, en lo concerniente al Modelo Integrado de Planeación y Gestión, y a la política de Gobierno Digital, del Ministerio de Tecnologías de la Información y las Comunicaciones.
- Definir e implantar controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, y perdida de integridad, que respondan a la disponibilidad requerida por los usuarios o clientes externos de la Entidad.
- Proteger la información a la que se acceda y procese, para evitar su perdida, alteración, destrucción o uso indebido.
- Registrar y monitorear las violaciones a las políticas y controles de seguridad de la información, y a su vez reportarlas a la Oficina de Talento Humano, para que dé inicio a las investigaciones pertinentes de conformidad con el control disciplinario interno y a lo establecido en el Código Único Disciplinario.

ARTÍCULO 5. PRINCIPIOS FUNDAMENTALES DE LAS PSI:

El sistema de gestión de seguridad de la información, preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo. Los siguientes son los conceptos sobre los cuales se diseñaron las Políticas Institucionales de Seguridad de la Información:

- **RESPONSABILIDAD EN LA CONTRATACIÓN E INDIVIDUALIZACION:**
  Este principio consiste en que cada persona es responsable de cada uno de sus actos, aun si tiene o no conciencia de las consecuencias.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

Identificar los riesgos asociados al acceso, procesamiento, comunicación o gestión de la información y/o la infraestructura para su procesamiento, por parte de personas o Entidades externas, terceros y/o contratistas, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Definir una cláusula de confidencialidad de la información, como parte integral de los contratos con personas o Entidades externas, terceros y/o contratistas, cuando deban tener acceso a la información y/o recursos de la Entidad; además, de no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información, teniendo en cuenta que cualquier violación a lo establecido en dicha cláusula será considerado como un "incidente de seguridad".

Incluir este documento como parte integral del procedimiento de Inducción y reinducción de la Entidad y de la Oficina de Sistemas e Informática de Indeportes Antioquia.

- **AUTORIZACIÓN:**
  Lo constituyen las reglas explícitas acerca de quién puede hacer qué. Es decir, de qué manera cada usuario puede utilizar los recursos informáticos.

  Los activos de información disponibles para los servidores públicos, contratistas y/o terceros, para su uso, operación y/o custodia, de acuerdo a las funciones específicas y necesidades del trabajo a realizar son propiedad exclusiva de la Entidad.

- **MÍNIMO PRIVILEGIO:**
  Este principio indica que cada usuario debe estar autorizado a disponer únicamente de los recursos que requiera para realizar su trabajo, de acuerdo a sus funciones o actividades contractuales. Acoger este principio, además de constituirse en una medida de seguridad, facilita además la prestación de los servicios por parte del personal de la Oficina de Sistemas e Informática.

- **SEPARACIÓN DE OBLIGACIONES:**
  Este principio establece que las actividades de un procedimiento deben ser distribuidas entre varias personas, con el fin de minimizar las posibilidades de error y/o ataques a la seguridad. Este principio facilita la aplicación de controles, el monitoreo y fortalece la transparencia administrativa.

- **AUDITORÍA:**
  Todas las actividades y todas las personas que intervienen en ellas deben poder ser auditadas, desde el inicio, hasta el final del proceso, e incluso, después de terminado, para garantizar que los datos no sean alterados durante o después de terminados los trámites.

- **REDUNDANCIA:**
  Este principio establece que la distribución y configuración de los recursos debe facilitar la restauración del servicio en caso de interrupciones fortuitas. Para eso, tanto los equipos como los programas y sus datos deben tener un respaldo. La configuración y el alcance de la redundancia se establece en el plan de contingencia y continuidad de la información. Se busca tener redundante lo que más afecte el servicio, por eso se configuran los servidores de autenticación como principal y secundario, se dispone de copias de respaldo por fuera de la Entidad y se establecen servicios en la nube, donde los proveedores garanticen su disponibilidad.

- **CONFIDENCIALIDAD:**
  La información no se pone a disposición ni se revela a individuos, Entidades o procesos no autorizados.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

- **INTEGRIDAD:**
  Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **DISPONIBILIDAD:**
  Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, Entidades o procesos autorizados cuando lo requieran.

ARTÍCULO 6. CONFIGURACIÓN DE LA RED CORPORATIVA:

La red Institucional deberá estar segmentada para independizarla según los usuarios, conexiones con terceros y del servicio de acceso a Internet y determinar las conexiones y servicios para los diferentes usuarios, terceros y personal externo (invitados).

Los servidores públicos y contratistas de la Entidad deberán estar siempre conectados a la red CORPORATIVA, inalámbrica y cableada.

ARTÍCULO 7. USO Y CUIDADO DE LOS ACTIVOS DE INFORMACIÓN:

La instalación de los equipos de cómputo (computadores, servidores, estaciones de trabajo, portátiles; impresoras; scanners; switches; AP´s, teléfonos; cables y puntos de red UTP), sean éstos propiedad de Indeportes Antioquia o en calidad de arrendamiento, sólo podrá realizarse por parte del personal de la Oficina de Sistemas e Informática de la Entidad, quien puede ser acompañado de personal técnico experto. Ningún usuario está autorizado para hacer, por su propia cuenta, ninguna reubicación de los equipos de cómputo a su cargo, ni tampoco puede hacer una reasignación de los mismos, sin el aval técnico de la Oficina de Sistemas e Informática; una vez se cuente con dicho concepto, se procederá a oficializar el traslado del bien con conocimiento del ALMACÉN.

Ningún usuario podrá retirar de las instalaciones los equipos asignados, excepto los computadores portátiles que cuenten con póliza de seguros con amparo móvil. A no ser que se presenten medidas excepcionales y el comité de gerencia autorice las mismas.

Cualquier tipo de conexión a la red ***CORPORATIVA*** de la Entidad ya sea cableado o wifi se realizará únicamente desde los equipos de cómputo asignados a los servidores públicos y/o contratistas por el personal de la oficina de Sistemas e Informática. Los equipos personales, así como los invitados, y deportistas podrán conectarse únicamente a las redes wifi disponibles para ellos.

La Oficina de Sistemas e Informática, realizará seguimiento y control anualmente al licenciamiento del software y aplicaciones de la Entidad.

Los usuarios no deben intentar, por su cuenta, hacer reparaciones a los equipos de cómputo. No están autorizados para instalar o para retirar partes de los mismos.

Cada usuario es responsable de apagar los equipos que estén a su cargo cuando finalice la jornada de trabajo.

Los usuarios deben bloquear su sesión durante los momentos en que se encuentre desatendido su computador, para evitar que personal ajeno usurpe su identidad y haga uso indebido de los recursos en su nombre o consulten información para la cual no están autorizados. El procedimiento bloqueo_de_pantalla se dicta en la inducción al personal**.** Además del bloqueo automático, está configurado un bloqueo automático después de diez (10) minutos de inactividad.

Los usuarios deben notificar a la Oficina de Sistemas e Informática, a través de la herramienta tecnológica "***mesa de ayuda***", (el procedimiento se dicta en la inducción al personal**.**), cualquier solicitud, incidente o problema con los recursos tecnológicos que

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

operan, quien gestionará la intervención de personal interno o externo para la solución de la situación reportada.

No debe colocarse elementos como plantas, bebidas o alimentos cerca a los equipos, ni bloquear las rejillas de ventilación.

En los tomas-regulados (color naranja) sólo deben conectarse los equipos de cómputo. En especial no pueden conectarse ventiladores, radios, tajalápiz a dichos circuitos por que causan interferencia que puede afectar el buen funcionamiento de los equipos.

Los equipos asignados a los usuarios deben ser utilizados solamente para actividades propias de INDEPORTES ANTIOQUIA. Sólo podrán usarlos para actividades personales o académicas tales como consultas de internet, redacción de documentos, capacitaciones virtuales, entre otros, durante la hora del almuerzo y antes o después de la jornada laboral ordinaria, siempre y cuanto estas actividades no atenten contra la seguridad, la confidencialidad, la disponibilidad de los recursos institucionales.

La Oficina de Sistemas e Informática, será la responsable de la identificación y clasificación de los activos de información, para establecer los mecanismos de protección correspondientes.

Se debe restringir el acceso a los documentos físicos y digitales según las normas aplicables internas y/o externas, y a los permisos determinados de acuerdo con las funciones del perfil de cargos.

Toda la información de los procesos de la Entidad, así como los activos donde ésta se almacena y se procesa están:

- Inventariados.
- Asignados a un responsable.
- Protegidos y clasificados; de acuerdo con la clasificación se deben establecer los niveles de protección orientados a determinar a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación

La Oficina de Sistemas e Informática, deberá revisar la identificación y la clasificación de los activos de información anualmente y/o cuando se presenten cambios que puedan afectar las mismas.

Se deberán proteger adecuadamente todos los equipos que hacen parte de la infraestructura tecnológica de la Entidad para prevenir la pérdida, el daño, robo o los accesos no autorizados; y ubicarlos alejados de sitios que puedan tener amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética, vandalismo, entre otros.

ARTICULO 8: INVENTARIO DE EQUIPOS.

La Oficina de Sistemas e Informática, lleva un registro de todos los equipos instalados en la red, donde especifica los datos básicos y guarda la relación con el usuario responsable. El ALMACÉN deberá hacer entrega formal del equipo al respectivo usuario y dejar registrada dicha entrega en un formato firmado por ambas partes, emitido desde el software ERP-Módulo Almacén/Inventarios/Activos fijos. El usuario debe verificar que el ALMACÉN le haga entrega de todos los elementos que componen el equipo y/o elemento que se reflejan en el documento firmado.

Cualquier daño en los computadores debe ser reportado a la mesa de ayuda de Sistemas para que sus técnicos procedan con su revisión; en caso de daño irreparable, el usuario afectado deberá informar al almacén para su reemplazo, quienes a su vez coordinan con Sistemas la nueva solución para el afectado.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

Los equipos de cómputo y demás elementos de tecnología quedan asignados a la cartera de cada servidor público y al supervisor de cada contratista quien será el único responsable y quien deberá garantizar el buen uso del mismo.

La Oficina de Sistemas e Informática, dispone del software INPACOM, donde lleva un registro pormenorizado del movimiento (asignación, traslado, cambio) y novedades que se va presentando con los equipos y dispositivos del parque computacional; constituyéndose en elemento de seguridad, control y apoyo a la gestión del almacén en material de circulación de los bienes tecnológicos.

ARTICULO 9. MANTENIMIENTO DE EQUIPOS:

Los equipos de la Entidad deberán estar asegurados contra todo riesgo, daño, pérdida o robo. Ante cualquier incidente de dicha naturaleza el servidor público informará inmediatamente a la Oficina de Sistemas e Informática, especificando el tipo, modo, tiempo y lugar del incidente para iniciar lo establecido en la política de activos de la Entidad.

El mantenimiento preventivo y/o correctivo de los equipos será programado por la Oficina de Sistemas e Informática y se realizará sólo bajo la supervisión de los servidores públicos de dicha Oficina.

ARTÍCULO 10. REUBICACIÓN DE EQUIPOS:

Los usuarios deben reportar a la Oficina de Sistemas e Informática, las necesidades de reubicación de equipos, quienes verificará las condiciones mínimas para su funcionamiento (punto de red, corriente regulada, seguridad física) en el nuevo sitio indicado.

El acceso a los equipos especializados conectados a la red (servidores, discos duros de respaldo, switches, AP´s, entre otros), es exclusivo para los servidores públicos y/o contratistas de la Oficina de Sistemas e Informática.

Ningún usuario está autorizado para manipular los elementos de red o comunicaciones situados en áreas públicas, o los que estén situados cerca a su puesto de trabajo. Si observa algo inusual, tal como ruido, fuego, desajustes, debe reportar inmediatamente a la “mesa de ayuda”.

ARTÍCULO 11. SOFTWARE:

La Oficina de Sistemas e Informática, con el apoyo de la Asesoría de Control Interno, son los responsables de asegurar que sólo el software con licencia esté instalado en los computadores de la Entidad.

Todo software que deba ser instalado en la plataforma institucional debe ser evaluado por la Oficina de Sistemas e Informática, sea éste en calidad de donación, prueba, convenio interinstitucional o instalación definitiva.

Los usuarios deberán reportar a la Oficina de Sistemas e Informática, las necesidades de software, con el fin de evaluar y tramitar el licenciamiento respectivo.

Los únicos servidores públicos y/o contratistas autorizados parar realizar instalación y desinstalación de programas, así como cambios de configuración en el Sistema Operativo, son los adscritos a la Oficina de Sistemas e Informática.

ARTÍCULO 12. CONTROL DE ACCESO:

La Oficina de Sistemas e Informática, es la encargada de crear los usuarios del dominio.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

El nombre del usuario del dominio Institucional se creará conformado por la inicial del primer nombre seguida por el primer apellido del respectivo usuario, en caso de que ya se encuentre creado un usuario que coincida con dichos valores, se buscará una combinación factible, usando el segundo nombre o apellido.

A los siguientes aplicativos Institucionales se accederá utilizando las credenciales del dominio de forma unificada:

- Acceso a la red.
- Office 365 (Correo electrónico, OneDrive, Skype empresarial y herramientas ofimáticas).
- Mesa De Ayuda.

Se definirán roles y responsabilidades, frente al nivel de acceso y los privilegios de los servidores públicos que tengan acceso a la infraestructura tecnológica y a los sistemas de información de la Entidad, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la Entidad.

Se implementarán reglas de control de acceso para todos los sistemas de disponibilidad crítica o media de la Entidad, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

Se establecerán controles duales sobre el nivel de súper usuario de los sistemas de información, de tal forma que exista supervisión a las actividades realizadas por el administrador del sistema.

Se deben establecer medidas de control de acceso físico en el perímetro que puedan ser auditadas, así como procedimientos de seguridad que permitan proteger la información, el software y el hardware de daños intencionales o accidentales para todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones.

ARTÍCULO 13. CONTROL DE ACCESO REMOTO:

La Oficina de Sistemas e Informática, es la única dependencia que puede autorizar el acceso remoto a los recursos de red cuando se requiera, para que los proveedores de los aplicativos específicos brinden asesoría, diagnostiquen la causa de algún mal funcionamiento, realicen labores de actualización de la plataforma o hagan algún ajuste en la configuración, indispensable para el buen funcionamiento y la disponibilidad de los servicios.

La Oficina de Sistemas e Informática, es la encargada de asignar las claves de acceso temporales y realizar la conexión con el proveedor respectivo.

Utilizar siempre cifrado de datos para las conexiones remotas a la infraestructura tecnológica de la Entidad, las cuales serán otorgadas de acuerdo con las necesidades de cada usuario y previa autorización del jefe del área correspondiente; será responsabilidad de cada usuario velar por la seguridad, confidencialidad e integridad de la información a la que tiene acceso de forma remota.

ARTÍCULO 14. ACCESO A LOS SISTEMAS DE INFORMACIÓN:

A los Sistemas de Información sólo tendrán acceso los usuarios de INDEPORTES ANTIOQUIA que sean titulares de una cuenta del dominio y que tengan la autorización del Área responsable de administrar el Sistema de Información en particular.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

Los jefes inmediatos de los servidores públicos o los supervisores de los contratistas, deben realizar las solicitudes de creación de usuario de los diferentes sistemas de la Entidad por medio del aplicativo “mesa de ayuda” de la Entidad, especificando las necesidades de acceso a los respectivos sistemas de información.

Una vez recibido y validado el requerimiento, se procede a crear y/o modificar el usuario. La Oficina de Sistemas e Informática, coordinará las capacitaciones a los usuarios para el ingreso y operación de la respectiva aplicación.

El control de acceso a cada Sistema de Información será determinado de acuerdo con la oficina responsable de generar y procesar los datos involucrados. Cada Jefe de Dependencia es el responsable de informar a la Oficina de Sistemas e Informática, cuando los usuarios terminen el vínculo laboral o contractual con la Entidad por medio del aplicativo de “mesa de ayuda”, indicando la fecha de retiro del servidor público o el contratista.

ARTÍCULO 15. GESTIÓN DE CONTRASEÑAS:

La Oficina de Sistemas e Informática, asignará una contraseña inicial que será informada al usuario para realizar el primer acceso al sistema. La primera vez que el usuario acceda a la red, deberá cambiar la contraseña, utilizando como mínimo seis (6) caracteres alfanuméricos y utilizando mínimo una letra mayúscula un número y un carácter especial. La vigencia de dicha contraseña será de 30 días, después de este período, el sistema solicitará cambio de contraseña. Durante el cambio de contraseña, el sistema no permite asignar la misma clave hasta después de seis (6) claves utilizadas previamente.

Las contraseñas de acceso a la red o de ingreso a los respectivos aplicativos (Intranet, Mercurio, ERP, entre otros) son de carácter personal e intransferible. El usuario se hace responsable del mal uso que pueda darse de los equipos o programas a su cargo, si divulga o deja en lugar público las contraseñas de acceso. Dicho de otra forma, los usuarios son responsables de todas las actividades realizadas con su cuenta de usuario del dominio o cuenta de aplicativos y sus claves personales.

La Oficina de Sistemas e Informática, podrá restablecer la contraseña de un usuario sólo mediante solicitud del propio usuario o mediante solicitud de su jefe inmediato o supervisor (Por medio de un requerimiento en la “mesa de ayuda”)

El jefe inmediato que autorizó el cambio de contraseña, debe notificarle al usuario cuando éste regrese a su sitio de trabajo, para que pueda ingresar nuevamente y proceder a asignar otra contraseña personal.

La vigencia de la cuenta de dominio está determinada por el tiempo de vinculación del usuario con la Entidad. La oficina de Sistemas e Informática, hará depuraciones periódicas para garantizar la desactivación de los usuarios que se desvinculan o terminan su contrato.

Todo usuario que utilice los recursos de los sistemas y de Red, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad, confiabilidad y auditabilidad de la información que maneje.

ARTÍCULO 16. PRIVILEGIOS DE NAVEGACIÓN:

Todos los usuarios de INDEPORTES estarán asociados a un GRUPO de navegación, el cual dispone de los servicios de internet requeridos de acuerdo a su cargo.

Los grupos establecidos en la Entidad son los siguientes:

- NAVEGACION_ORO
- NAVEGACION_PLATA
- NAVEGACION_BRONCE

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

Cada grupo tiene configurado un perfil que le asigna las categorías permitidas, los horarios en los cuáles se conceden privilegios de consulta adicionales y las URL específicas de ciertas categorías no permitidas que se autorizan, de acuerdo a los requerimientos institucionales.

Por defecto todos los usuarios se asignarán al perfil bronce a excepción de los directivos que se asignarán al perfil ORO. En caso de requerir permisos adicionales de navegación, el jefe directo del servidor público deberá realizar el respectivo requerimiento en la "mesa de ayuda" de la Entidad, indicando el perfil al cual se debe asociar el usuario.

La configuración de los grupos es dinámica y se actualiza conforme a las necesidades Institucionales y a las actividades particulares asignadas a los usuarios, con la debida sustentación de la necesidad.

Los usuarios no podrán consultar o actualizar las redes sociales o sitios de *streaming* de audio y video por fuera de los horarios autorizados por la administración, excepto los que por razón de sus actividades institucionales, estén encargados de dicha actividad.

ARTÍCULO 17. SERVIDOR DE ARCHIVOS (FILE SERVER):

La Entidad dispone de un servidor exclusivo para almacenar información de:

- Oficinas que manejan información compartida.
- Respaldo de la información de servidores públicos retirados.
- Respaldo de buzones de correo de servidores públicos retirados entre otras.

La información de trabajo de todos los usuarios deberá ser almacenada en la carpeta personal de One Drive asignada con su cuenta de Office. Nunca se deberá almacenar información en el disco local del computador.

ARTÍCULO 18. PROTECCIÓN PERMANENTE CONTRA SOFTWARE MALICIOSO:

Todos los recursos informáticos estarán protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brinden protección contra los diferentes tipos de amenazas actuales.

Será responsabilidad de la Oficina de Sistemas e Informática, velar por la instalación y uso de las herramientas de seguridad, así como de su actualización permanente. Ningún usuario podrá deshabilitar o desinstalar bajo ninguna circunstancia dichos aplicativos.

Los usuarios deberán hacer revisión de virus a los discos y memorias externas antes de copiar o abrir archivos y no deben interrumpir los procesos de escaneo que se configuren automáticamente en la máquina, como mecanismo de detección y protección. Este proceso de escaneo automático se realiza por políticas de grupo de administración periódicamente todos los viernes a partir de las 12:00 p.m. y hasta las 2:00 p.m. aproximadamente.

Está totalmente prohibido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

ARTÍCULO 19. CONTENIDO PÁGINA WEB E INTRANET:

La Oficina Asesora de Comunicaciones, es la responsable de realizar las publicaciones en los diferentes portales de la Entidad, y por tanto debe revisar todo el material que deba ser publicado en la Página Web o en la Intranet y realizar los ajustes de estilo pertinentes.

También le corresponde a ésta Oficina, en concordancia con la Oficina de Sistemas e Informática, generar reglas de seguridad para las redes sociales (twitter, Facebook, Youtube, Instagram, LinkedIn etc.), por ej. tener el doble factor de autenticación habilitado

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

y otras más que permitan blindar, el activo vital de nuestra Entidad; como lo es la información publicada.

El usuario que genere cada contenido debe velar por el respeto de la ley de derechos de autor, hacer las citas que referencien material creado por terceros y tramitar las autorizaciones pertinentes para citar, referenciar o hacer hipervínculos a dichos contenidos. Se debe cumplir con los mismos requisitos que se aplican a los contenidos impresos.

Cada área de la Entidad es responsable por la publicación de la información requerida de acuerdo con la ley de transparencia y acceso a la información pública.

ARTÍCULO 20. CORREO ELECTRÓNICO INSTITUCIONAL:

Todos los usuarios de la Entidad, deberán enviar la información corporativa exclusivamente desde la cuenta de correo que la Oficina de Sistemas e Informática proporciona.

La cuenta de correo electrónico institucional será solicitada por medio de la plataforma “mesa de ayuda”, por el jefe directo del servidor público o contratista, o en quien este designe dichas funciones. En dicha comunicación se debe detallar el nombre (cédula de ciudadanía), dependencia donde labora o presta sus servicios la persona a la cual se le va asignar la cuenta. De igual manera, el jefe del Área debe informar, cuando la cuenta del usuario deba ser desactivada.

El usuario del correo institucional (usuario), coincidirá con el usuario del dominio, descrito anteriormente.
La cuenta de correo estará conformada de la siguiente forma: (*usuario*@indeportesantioquia.gov.co).

El tamaño de los buzones de correo electrónico es de 50 Gb; si un usuario requiere espacio adicional, deberá solicitarlo a la Oficina de Sistemas e Informática, quien determinará, la posibilidad de aceptar o no la solicitud.

Solo se podrán enviar y/o recibir correos electrónicos que tengan un peso máximo de 30 Mb.

Todas las listas de Distribución serán creadas y configuradas por la Oficina de Sistemas e Informática, previa solicitud de la Oficina de Comunicaciones o la Oficina de Talento Humano; todas las firmas predeterminadas y pie de página de los correos electrónicos, serán diseñadas y configuradas por la Oficina de Comunicaciones e implantadas por la Oficina de Sistemas e Informática.

Algunas áreas o proyectos que requieran un correo electrónico de uso genérico, deberán solicitarlo a la Oficina de Sistemas e Informática, por medio de la plataforma “mesa de ayuda”. Es responsabilidad del jefe de Área y podrán designar la atención de dicha cuenta de correo a un servidor público de su dependencia, sin eximirse de la responsabilidad por el cumplimiento de las presentes normas e independientemente del accionar del personal en el cual delegue tales funciones.

La cuenta de correo asignada a un usuario es personal e intransferible. Queda estrictamente prohibido intentar o apoderarse de claves de acceso de otros usuarios, acceder y/o suplantar la identidad de otro usuario. Ningún usuario está autorizado para divulgar su clave a otros y permitir que ellos hagan en su nombre tareas que están bajo su responsabilidad.

Queda estrictamente prohibido el uso del correo electrónico Institucional para divulgar información confidencial de la Entidad o información catalogada como sensible. Esta prohibición se extiende a los correos de carácter personal, es decir, ni el correo institucional

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

ni el personal pueden usarse como medio para divulgar información Institucional de carácter sensible.

Queda estrictamente prohibido el uso del correo electrónico Institucional para cualquier propósito delictivo, comercial, financiero, político, religioso o temas similares, ni para atentar contra el buen nombre de Instituciones o personas.

Se debe tener en cuenta que el uso de los correos personales y las redes sociales usando los canales Institucionales, también comprometen a la Entidad, pues nuestras direcciones de internet podrían quedar en listas negras y afectar esto las condiciones de prestación de servicio.

Los usuarios no podrán utilizar el correo institucional para suscripciones a servicios o envío de correos personales comerciales.

No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, xenófobo, homófobo, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y/o la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Entidad; de igual forma mensajes malintencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico corporativa como punto de contacto en comunidades interactivas de contacto social, tales como facebook y/o Twitter o cualquier otro sitio que no tenga que ver con las actividades laborales.
- Enviar archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- Enviar y/o recibir archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la mesa de ayuda de INDEPORTES.
- Entregar la lista de correo electrónico de los servidores públicos de la Entidad, a usuarios externos que la utilicen para fines comerciales o políticos.
- Abrir correos electrónicos de remitentes desconocidos o que sean sospechosos de tener contenido malintencionado como virus o malware.
- Intercambiar información no autorizada de propiedad de INDEPORTES y/o de sus usuarios con terceros.
- Los usuarios no podrán utilizar el correo institucional para suscripciones a servicios o envío de correos personales o comerciales.
- Queda estrictamente prohibido el uso del correo electrónico institucional, para propagar mensajes de tipo cadena, no importa el contenido del mensaje divulgado. Si nuestra Institución recibe quejas, denuncias o reclamaciones por estas prácticas, se tomarán las medidas disciplinarias pertinentes.

ARTÍCULO 21. INTERNET:

Se controlará, verificará y monitorear para el uso y la navegación en internet de todos los usuarios conectados a la red de la Entidad de manera permanente, con el fin de garantizar el uso eficiente del canal corporativo y mantener la seguridad de la información.

La Oficina de Sistemas e Informática, podrá en cualquier momento inspeccionar los tiempos de navegación, páginas visitadas y evaluar las actividades realizadas durante la navegación de acuerdo a la legislación nacional vigente por los usuarios de la Entidad en los canales institucionales.

La Entidad reconoce que los usuarios de la red pueden usar esporádicamente los recursos de internet que les han sido asignados, o a los que tienen acceso, para uso personal y

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

ocasional, pero nunca para uso comercial. Los canales de internet institucionales no deben usarse para promover sistemas multiniveles como: esquemas de pirámide, o conducir a rifas o sorteos en los que haya que pagar por el acceso. Tal uso personal y ocasional no debe ser excesivo y no debe interferir con la operación eficiente de los canales y servicios de la Institución, ni con los deberes y obligaciones de las personas establecidas en los diferentes reglamentos y manuales.

Está prohibido descargar intercambiar, usar y/o instalar música, juegos, películas, fondos de pantalla que cambien lo institucional, software de libre distribución, información y/o productos que atenten contra la propiedad intelectual o cualquier otro software que comprometan la integridad y disponibilidad de la plataforma tecnológica de la Entidad.

Está prohibido consultar páginas de carácter pornográfico o sexual, violencia en línea, software ilegal, drogas, alcohol, hacking y/o cualquier otra página que vaya en contra de la ética, las leyes vigentes o políticas establecidas en el presente documento

Está prohibida la consulta de las páginas de redes sociales o de *streaming* de audio y video durante la jornada laboral, excepto para el personal que actualiza Información Institucional en estos sitios o que por su perfil requiera acceso permanente a dichos sitios para consulta de información ligada con sus funciones. No obstante, el acceso a dichos sitios sí estará permitido para los demás usuarios en horario determinado:

> Antes del inicio de la jornada laboral, desde las 6:00 a.m. hasta las 7:30 a.m. De las 12 m. hasta la 1:00 p.m., y después de la jornada laboral desde las 5:30 p.m. hasta las 10:00 p.m. (Los viernes desde las 5:00 p.m.), siempre y cuando su utilización no viole las disposiciones de seguridad y la normatividad vigente.

Se prohíbe la distribución intencional de virus, gusanos, troyanos o la realización de cualquier tipo de actividad destructiva en calidad de hacker o similar.

Se prohíbe usar los servicios de la red para propósitos fraudulentos o para la propagación de mensajes destructivos u obscenos.

ARTICULO 22. OPERACIONES BANCARIAS VIA INTERNET.

Nuestra gestión en seguridad informática exige conexiones seguras, con prácticas como direcciones IP estáticas propias de nuestra red local, control de firewall, políticas de seguridad en dominio, plataformas web con certificaciones de seguridad, acceso al aplicativo con doble factor de autenticaciones, cifrado extremo – extremo y adhesión de clavija o centinela entre otros.

ARTÍCULO 23. COPIAS DE SEGURIDAD:

Asegurar que la información con cierto nivel de clasificación, contenida en la plataforma tecnológica de la Entidad, como servidores, dispositivos de red para almacenamiento, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Mantener un plan de restauración de copias de seguridad y revisarlo periódicamente, con el fin de asegurar que las copias sean confiables en caso de emergencia y retenidas por un periodo determinado.

Definir conjuntamente con equipo de gestión documental y de acuerdo a lo determinado por la ley, los períodos de retención de las copias de seguridad y disponer de los recursos necesarios para identificar los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos, permitiendo un rápido y eficiente acceso a los medios que contienen la información resguardada.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

Almacenar en un sitio externo los medios magnéticos que contienen las copias de seguridad de la Entidad; dicho sitio debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiada.

Asegurar el servicio de sincronización en la nube (onedrive), de la información que se encuentre en las carpetas Mis Documentos, Mis Imágenes, en el Escritorio o carpetas propias de la nube en el equipo de los usuarios. Información almacenada en una ubicación diferente no será respaldada.

Excluir del proceso de respaldo los archivos con extensiones .exe, .mp3, entre otras similares.

ARTICULO 24. SEGURIDAD DE LA INFORMACIÓN PARA LOS MEDIOS EXTRAÍBLES:

Implementar los controles necesarios para asegurar que en los equipos de cómputo institucionales sólo los servidores públicos y contratistas autorizados puedan hacer uso de los medios de almacenamiento extraíbles.

Asegurar física y lógicamente los dispositivos extraíbles con el fin de no poner en riesgo la información de la Entidad contenida en los mismos.

ARTÍCULO 25. SERVICIOS DE IMPRESIÓN:

La Entidad tiene distribuido el servicio de impresión en zonas, que permiten a los usuarios utilizar por defecto la impresora más cercana a su puesto de trabajo, todas ellas están en red, de manera que los usuarios pueden usar otra, en caso de alguna falla o situación atípica de congestión en su dependencia.

Cada impresora es en realidad un equipo multifuncional que permite además copiar, escanear y enviar las imágenes al correo electrónico.

Los usuarios tienen asignada una contraseña por medio de la cual pueden utilizar los servicios, la cual se digita en el panel de control del respectivo multifuncional.

La información sensible que se envía a las impresoras se debe recoger de forma inmediata.

La Entidad, por medio de la Resolución S 202000406 del 03 de julio de 2020, ordenó adoptar e implementar en INDEPORTES las buenas prácticas del uso del papel orientadas a la implementación de la Política Cero Papel, por medio del aprovechamiento, de las tecnologías de la información y comunicaciones TIC aplicando los principios de *Gestión Documental*.

Como gestión en esta política, la Entidad tiene implementada la plataforma MERCURIO, sistema que cumple a cabalidad e integra en su total el flujo de documentos basado en procesos, rutas y workflow con cobertura total de transversalidad.

ARTÍCULO 26. SUPERVISIÓN ENTREGA INFORMACION CONTRATISTAS:

Las Oficinas Talento Humano u Oficina Asesora Jurídica o en defecto el supervisor del contrato, notificarán a la Oficina de Sistemas e Informática, por medio de la “mesa de ayuda” los servidores públicos y/o contratistas que ingresarán a la Entidad indicando su cargo y perfil o labor, nombre completo y número de documento de identidad, el tipo de equipo, aplicativos y permisos a asignar, la fecha de ingreso y su ubicación; La Oficina de Sistemas e Informática contará con un máximo de cinco (5) días hábiles para asignar lo requerido; de igual forma, deberán notificar y con una anticipación de cinco (5) días hábiles el retiro del servidor público y/o contratista, para realizar las respectivas copias de seguridad y la desactivación del usuario.

ARTÍCULO 27. SEGUIMIENTO:

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

La Oficina de Sistemas e Informática, monitoreará de forma permanente que los sistemas y recursos de la red operen adecuadamente y que los usuarios estén acatando las directrices emanadas en este documento.

La Oficina de Control Interno realizará auditorías internas para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a este documento y para analizar y planificar acciones de mejora.

ARTÍCULO 28. GENERALIDADES:

Todos los usuarios de INDEPORTES ANTIOQUIA son responsables del cumplimiento de cada una de las políticas de seguridad y los jefes de las dependencias deberán supervisar el cumplimiento de las mismas.

ÁRTICULO 29. MARCO NORMATIVO:

- ***Ley 23 de 1982 –*** *Sobre Derechos de Autor.*

- ***Ley 599 de 2000 -*** *Código Penal*

- ***Ley 1032 de 2006*** *- Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal:* ***Artículo*** *257. De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos.* ***Artículo*** *272. Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones.*

- ***Ley 679 de 2001*** *- Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.*

- ***Ley 1273 de 2009 -*** *El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*

- **SANCIONES:**
  Ante la evidencia del incumplimiento de lo establecido en el presente documento, la administración podrá iniciar los procesos disciplinarios a que haya lugar o aplicar las sanciones administrativas correspondientes, o dar traslado a la autoridad competente para que se haga la respectiva investigación de tipo penal, de acuerdo con la normatividad vigente.

  A continuación, se referencia algunas de las sanciones establecidas por la Ley:
  La protección de la Información y de los Datos, está contemplada en el código penal, a través de la **Ley 1273 del 5 de enero de 2009**, con la que se pretende preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones penalizando conductas inapropiadas y sancionándolas penalmente:

  *- **Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO:** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. *El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.*

- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. *El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.*

- Artículo 269D: DAÑO INFORMÁTICO. *El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

- Artículo 269E: USO DE SOFTWARE MALICIOSO. *El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

*- **Artículo 269F: VIOLACIÓN DE DATOS PERSONALES.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

- ***Ley 679 de 2001: ARTÍCULO 7o. PROHIBICIONES.*** *Los proveedores o servidores, administradores y usuarios de redes globales de información no podrán:*
1. Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad.

2. Alojar en su propio sitio material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad.

3. Alojar en su propio sitio vínculos o links, sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad.

ARTÍCULO 10. SANCIONES ADMINISTRATIVAS. *El Ministerio de Comunicaciones tomará medidas a partir de las denuncias formuladas, y sancionará a los proveedores o servidores, administradores y usuarios responsables que operen desde territorio colombiano, sucesivamente de la siguiente manera:*

1. Multas hasta de 100 salarios mínimos legales vigentes.

2. Cancelación o suspensión de la correspondiente página electrónica.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

Para la imposición de estas sanciones se aplicará el procedimiento establecido en el Código Contencioso Administrativo con observancia del debido proceso y criterios de adecuación, proporcionalidad y reincidencia.

PARÁGRAFO. El Ministerio de Comunicaciones tendrá competencia para exigir, en el plazo que este determine, toda la información que considere necesaria a los proveedores de servicios de internet, relacionada con la aplicación de la Ley 679 y demás que la adicionen o modifiquen. En particular podrá:

1. Requerir a los proveedores de servicios de internet a fin de que informen en el plazo y forma que se les indique, qué mecanismos o filtros de control están utilizando para el bloqueo de páginas con contenido de pornografía con menores de edad en Internet.

2. Ordenar a los proveedores de servicios de internet incorporar cláusulas obligatorias en los contratos de portales de internet relativas a la prohibición y bloqueo consiguiente de páginas con contenido de pornografía con menores de edad.

Los proveedores de servicios de internet otorgarán acceso a sus redes a las autoridades judiciales y de policía cuando se adelante el seguimiento a un número IP desde el cual se produzcan violaciones a la presente ley.

***ARTÍCULO 35.** Adicionase un nuevo artículo al Código Penal, con el número 312B, del siguiente tenor:*

***Artículo 312B. Omisión de denuncia.** El que, por razón de su oficio, cargo, o actividad, tuviere conocimiento de la utilización de menores para la realización de cualquiera de las conductas previstas en el presente capítulo y omitiere informar a las autoridades administrativas o judiciales competentes sobre tales hechos, teniendo el deber legal de hacerlo, incurrirá en multa de diez (10) a cincuenta (50) salarios mínimos legales mensuales vigentes.*

Si la conducta se realizare por servidor público, se impondrá, además, la pérdida del empleo.

***Ley 1336 de 2009:** La Ley 1336 de 2009 especifica en su Capítulo VI, artículo 24, una modificación al artículo 218 de la ley 599, referente a la pornografía con personas menores de 18 años:*

***Artículo 218.* Pornografía con personas menores de 18 años.** *El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes.*

Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.

La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.

ARTÍCULO 30. COMUNICACIÓN:

El jefe de la Oficina de Sistemas e Informática, dará a conocer este documento por todos los medios de comunicación internos: Correo electrónico, Intranet y SharePoint y hacer firmar de cada uno de los usuarios el documento de compromiso con estas políticas: Acuerdo de uso de recursos informáticos.

Radicado: S 2020000514
Fecha: 10/09/2020
Tipo: RESOLUCIONES
Destino: No registra.

De igual forma, se realizarán campañas de sensibilización y jornadas de capacitación al personal de INDEPORTES, para fortalecer y mejorar la conciencia de auto cuidado y de seguridad de la información.

ARTICULO 31. REVISIÓN:

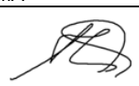
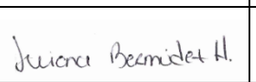
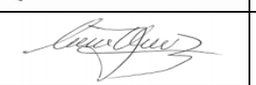
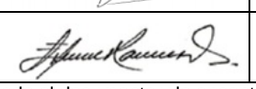
Esta resolución será revisada de forma anual por la Oficina de Sistemas y la alta Dirección de la Entidad, o antes si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

ARTÍCULO 32. VIGENCIA:

La presente resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

SERGIO ROLDÁN GUTIERREZ
Gerente

	NOMBRE	FIRMA	FECHA
Proyectó	Raúl Álvaro Ossa Gómez - Técnico Administrativo Oficina de Sistemas e Informática		07/09/2020
Revisó	Diana Marcela Ospina Rojas – Abogada contratista		08/09/2020
Revisó	Juliana Bermúdez Henao – Jefe Oficina de Sistemas e Informática		08/09/2020
Revisó	César Augusto Orozco Muñoz – Profesional Universitario Oficina Asesora Jurídica		09/09/2020
Aprobó	Luz Helena Ramírez Giraldo – Jefe Oficina Asesora Jurídica		09/09/2020
	Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.		